REMARKS

The Examiner is thanked for the comments in the Action. They have helped us considerably in understanding the Action and in drafting this Response thereto.

It is our understanding that claims 1-26 remain pending in this application, wherein claims 1, 5, 11, 14, 20, and 22 have been amended for reasons specifically remarked upon, below. **We proceed now with reference specifically to the numbered items in the Action.**

Item 1: This appears informational in nature and is understood to require no reply.

Item 2 (Hyperlink):

The Action here objects to the disclosure "*because it contains an embedded hyperlink and/or other form of browser-executable code (SPEC: Page 3 Para [0011]).*" Responsive hereto, paragraph [0011] has been amended.

Items 3-6 (objections):

Claims 1, 5, 11, 14, 20 and 22 are objected to because of informalities. Responsive hereto these claims are amended. No new subject matter is added by these amendments.

Item 7 (§ 101 rejection):

Claim 1 is rejected because it is directed to "*A computer program*" without limitation to such being stored on a computer readable storage medium. Responsive hereto, this claim is amended. No new subject matter is added by this amendment.

Item 8 (§ 103(a) rejections 1/4):

Claims 1, 3, 4, 6-9, 11-13, 15-18, 20, 21 and 23-25 are rejected as unpatentable (obvious) over Le Berre in view of Schneider. Respectfully this is error.

As a preliminary point, it has apparently not been appreciated that the claimed invention protects computer users from relying on malicious actions by other computer users, whereas Le Berre facilitates computer users automatically accessing resources distributed across multiple server computers and whereas Schneider protect computer users from computer or network malfunction. Both Le Berre and Schneider pertain to contexts where human malice is simply irrelevant.

Le Berre and Schneider, individually or in combination, cannot support a prima facie case for obviousness, and that can particularly be seen here by considering the initial assertion in item 8 of the Action as it discusses claim 1.

The Action states *"Le Berre teaches* ***a computer program for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed*** *(Le Berre: Abstract, the last sentence and Column 5 Line 56-58).*" Respectfully, this is simply wrong.

First, what a hyperlink is and contains appear to have been overlooked. A hyperlink is a reference or navigation element in a document, here a message. In the context of hyperlinks that potentially can be spoofed, a traditional hyperlink includes both a human interpretable element and a computer interpretable element. If the computer interpretable element points to what the human interpretable element indicates, all is fine. If the computer interpretable element points elsewhere, this can be due to innocent error or malicious human intent. Both Le Berre and Schneider deal with innocent error aspects, not with malicious human intent aspects.

The Action cites the last sentence of Le Berre's Abstract, but this merely states "*Information can also be included in the URI and the signature used at the second server (40B) to check its integrity.*" This refers to structural integrity, and that should not be confused with moral integrity. When the hull of a boat lacks structural integrity, the boat sinks. When a URL reads "*httq:/\w w w.somewhere.c 0 m*" it lacks structural integrity and does not function. In contrast, the people who create spoofed hyperlinks lack moral integrity. They seek to steal privileged information from or disrupt the lives of other people. But, unless such miscreants are also incompetent, the spoofed hyperlinks that they create have structural integrity. The sorry fact is that spoofed hyperlinks work and that is why the present invention is needed.

The above citation in the Action, to col. 5, ln. 56-58 (paragraph [0022]), also does not support the assertion or the overall point it appears the Examiner is trying to make.

First, nothing in the citation even suggests hyperlinks in the manner of the present invention. As described, a spoof-able traditional hyperlink includes both human and machine interpretable elements. As a very simple example, one e-mail might contain the HTML hyperlink:

"*<a href="http://www.uspto.gov/ebc/indexebc.html">Patent Office eBusiness</a>*"

and another (spoofed) e-mail might contain the HTML hyperlink

"*<a href="http://www.sex.com/ImageMenu.html">Patent Office eBusiness</a>*".

The text "*Patent Office eBusiness*" is the human interpretable element in both hyperlinks (it is al that will be humanly viewable unless special measurers are taken) and the rest is machine interpretable. In [0022] Le Berre does not teach or reasonably suggest anything about hyperlinks having human and machine interpretable elements. As its title states ("Authentication Between Servers") and as can be seen in its Fig. 4, Le Berre teaches and uses only machine interpretable elements. That is, it teaches URLs, rather than operations on hyperlinks containing URLs.

Digressing now to relate all of this to Applicant's invention, we stated above that "*a spoof-able traditional hyperlink includes both human and machine interpretable elements*." Simplistically stated, the present invention works by adding a new element to a hyperlink and providing code or logic that works with that. In claim 1 the "originator identifier" is the human interpretable element, the "target URL" is the machine interpretable element, and the "encrypted data" is the new element. Of course, many technologies put encrypted data in hyperlinks and URLs (Le Berre is an example). But claim 1 must be considered as a whole, taking into account all of the limitations it recites, and here is where Applicant's "encrypted data" is different and is used differently. Claim 1 recites "*a code segment that extracts an originator identifier and encrypted data from the hyperlink*," meaning that both are present together in the hyperlink (with the target URL), and claim 1 next recites "*a code segment that decrypts said encrypted data into decrypted data <u>based on</u> said originator identifier*" (underlining added for emphasis). The "originator identifier" is human interpretable, and thus typically not machine interpretable, but it is present and the machine/computer nonetheless "sees" it as a text or bit string. The machine/computer typically cannot understand what the "originator identifier" will signify to a human, but it can use the text or bit string as a cryptography key (or a basis to obtain such) to decrypt the "encrypted data." Note, since Applicant's "encrypted data" is tied to its "originator identifier," Applicant's "encrypted data" is not just any encrypted data (e.g., its is not Le Berre's crypto-signature).

Returning again to Le Berre and Schneider, and their combination, these do not teach or reasonably suggest an equivalent to Applicant's "originator identifier" and the use of one in the manner of the claimed invention, and these also do not teach or reasonably suggest an equivalent to Applicant's "encrypted data."

With the above as background, it can now be seen that the rest of the assertions in the Action are generalizations that are correct but non-determinative or that are also error. For example, continuing with respect to claim 1, the Action indicates that Le Berre teaches "***a code segment that listens with a computerized system for an activation of the hyperlink*** *(Le Berre: Column 7 Line 28-27* [SIC] *and Column 5 Line 56-58: an activation of the URL link).*" This is incorrect. The cited portions of Le Berre teach a prompt and response scenario, not “listening” for activation of a hyperlink. It appears that activation of an URL, a direct command, and listening/monitoring for a direct command to another entity have been confused here. Le Berre simply teaches going to a URL, rather than listening for a hyperlink, performing actions based on what is "heard," and then going to a URL.

Continuing with respect to claim 1, the Action indicates that Le Berre teaches:

> ***a code segment that extracts an originator identifier and encrypted data from the hyperlink*** *(Le Berre: Figure 5 and Column 6 Line 31-55, Column 10 Line 31-32, Column 12 Line 56 - Column 13 Line 1-5 and Column 3 Line 42-45: (a) the originating server ID is qualified as an originator identifier and (b) a data element is encrypted at the originate server A by using its private key and (c) the receiving server B decrypts the data and checks the received signature from within the qualified set of servers);*

This is incorrect in part, correct but not determinative in part, and illogical in part.

In Fig. 5 and at col. 6, ln 31-55 Le Berre teaches the use of a hash, not decryptable data. While hashing can be used in place of or with cryptography in some situations, that is not relevant here. As is well know, hashes operate one way and a copy of original data before being hashed cannot be recovered form the hash result. One of ordinary skill in the art will appreciate that claim 1 employs decryption and that hashed data cannot be substituted for Applicant's "encrypted data."

In col. 10, ln. 31-32 Le Berre teaches that encrypted data can be used in place of a hash. This is correct but not determinative here, since claim 1 must be considered as a whole and what Le Berre and Applicant use for the respective basis for decryption are different. Note also, Le Berre admits here that using encrypted data in place of a hash is not part of its preferred embodiment. Unstated here, but well known in the art, using encrypted data in place of a hash reduces security. By its very definition encrypted data can be decrypted, whereas hashed data cannot be de-hashed.

As for "*Column 12 Line 56 - Column 13 Line 1-5 and Column 3 Line 42-45*," we presume the Examiner means col. 12, ln. 56 through col. 13, ln. 5 and col. 3, ln. 42-45. If so, however, these do not recite an "*originating server ID*" or an "*originator identifier*," or qualifying anything (much less the former as the latter, which still would have no relevance here; note, claim 1 does not recite a code segment for qualifying). Similarly, the discussion of Le Berre's A and B servers and checking that a signature is for one of a qualified set of servers is not relevant. Claim 1 does not recite any servers, and especially not a set of "qualified" ones.

We could odiously go on with this with respect to Le Berre, but we urge that Applicant's point has been made. It does not teach or reasonably suggest what it has been relied upon for to support a rejection here based on the combination of Le Berre and Schneider.

The Action states "*Le Berre does not disclose expressly a code segment that presents information on a display unit...*" and in the next paragraph states "*Schneider in view of Le Berre teaches* ***a code segment that presents information on a display unit*** *(Schneider: Column 29 Line 9-13).*" First, the text "*Schneider in view of Le Berre teaches*" is nonsense. Schneider either teaches something or it does not. Second, this is illogical. It states that Le Berre does not disclose something, then asserts that Schneider in view of Le Berre does. Third, the cite to Schneider here is not determinative of anything. Many references teach presenting information on a display. The cited portion of Schneider here teaches teach presenting information on a display during a user registration dialog, i.e., the last thing or at least a totally irrelevant thing for a user to be doing in the context of Applicant's claim 1.

Continuing, here in the middle of a discussion supposedly about Schneider, the Action next states "***runs said code segment that presents, to present a confirmation of authentication to the user*** *(Le Berre: Column 8 Line 48-51).*" Firstly, this apparently is not a simple error where Schneider was meant instead. At col. 8, ln. 48-51 Schneider discusses search engine search results, and that is clearly irrelevant here. Secondly, what Le Berre teaches at col. 8, ln. 48-51 is returning a customer license number. But what possible relevance is this to detecting spoofed hyperlinks?

Similarly, we could odiously go on with this with respect to Schneider, but we urge that Applicant's point has been made. Schneider does not teach or reasonably suggest what it has been relied upon for to support a rejection here based on the combination of Le Berre and Schneider.

As per claims 11 and 20, these are system (apparatus) and method equivalents of claim 1, their rejections are also based on the combination Le Berre and Schneider, and we urge that these are therefore allowable for the same reasons as claim 1.

As per claims claims 3, 4, 6-9, 12-13, 15-18, 21 and 23-25, these all depend from claim 1, 11, or 20 and therefore should be allowable for the same reasons.

Item 9 (§ 103(a) rejections 2/4):

Claim 2 is rejected as being unpatentable (obvious) over Le Berre in view of Schneider and Dunnion. Respectfully this is error.

The combination Le Berre and Schneider do not support the rejection of parent claim 1, and the addition of Dunnion to this combination does not remedy this or support a prima facie case here.

Item 10 (§ 103(a) rejections of claims 3/4):

Claims 5, 14 and 22 are rejected as being unpatentable (obvious) over Le Berre in view of Schneider and Perry. Respectfully this is error.

The combination Le Berre and Schneider do not support the rejection of parent claims 1 and 20, and the addition of Perry to this combination does not remedy this or support a prima facie case here.

Item 11 (§ 103(a) rejections 4/4):

Claims 10, 19 and 26 are rejected as being unpatentable (obvious) over Le Berre in view of Schneider and Haitsuka. Respectfully this is error.

The combination Le Berre and Schneider do not support the rejection of parent claims 1, 11, and 20, and the addition of Haitsuka to this combination does not remedy this or support a prima facie case here.

Item (Conclusion):

This appears informational in nature and is understood to require no reply.

CONCLUSION

Applicant has endeavored to put this case into complete condition for allowance. It is thought that the objections and §101 rejections have all been corrected by amendment, and that the §103 rejections have also been addressed by amendment or have been completely rebutted. Applicant therefore asks that all objections and rejections now be withdrawn and that allowance of all claims presently in the case be granted.

Patent Venture Group
10788 Civic Center Drive, Suite 215
Rancho Cucamonga, California 91730-3805

Respectfully Submitted,

E. Roberts

Raymond E. Roberts
Reg. No.: 38,597

Telephone: 408.558.9950
Facsimile: 408.558.9960